

WHAT IS CLAIMED IS:

- 1 1. A network device comprising:
2 a tunnel classification stage.
- 1 2. The network device of claim 1, wherein said tunnel classification stage
2 comprises:
3 a packet processing section, configured to classifying a packet based on a
4 security group identifier (SGI) of said packet.
- 1 3. The network device of claim 2, wherein
2 said packet processing section is configured to forward said packet through a
3 tunnel on which said packet is to be conveyed based on said SGI.
- 1 4. The network device of claim 3, wherein
2 said packet processing section is further configured to forward said packet
3 through said tunnel based on information in a header of said packet.
- 1 5. The network device of claim 2, wherein said tunnel classification stage
2 further comprises:
3 a security group identifier identification unit, coupled to said packet processing
4 section; and
5 a tunnel classification unit, coupled to said packet processing section and said
6 security group identifier identification unit.
- 1 6. The network device of claim 1, wherein a router comprises said tunnel
2 classification stage.
- 1 7. The network device of claim 6, wherein said router further comprises:
2 a lookup unit.
- 1 8. The network device of claim 7, wherein said lookup unit comprises:
2 an access control list (ACL); and
3 a content-addressable memory, wherein

4 said content-addressable memory is coupled to said access control list,
5 and
6 said content-addressable memory is configured to generate an index
7 and to provide said index to said ACL.

1 9. The network device of claim 8, wherein said ACL comprises:
2 a plurality of ACL entries (ACEs), wherein
3 each of said ACEs comprises a tunnel identifier field and a security
4 group identifier field.

1 10. A method comprising:
2 assigning a security group identifier (SGI) to a packet; and
3 classifying said packet based on said SGI.

1 11. The method of claim 10, further comprising:
2 determining whether said packet can be sent via a tunnel based on a result of
3 said classifying said packet.

1 12. The method of claim 11, further comprising:
2 determining a routing of said packet, wherein said determining whether said
3 packet can be sent via said tunnel is also based on said routing.

1 13. The method of claim 12, further comprising:
2 forwarding said packet via said tunnel, if forwarding a packet having said SGI
3 via said tunnel is permitted.

1 14. The method of claim 11, wherein said determining comprises:
2 generating an index, wherein said index comprises said SGI; and
3 using said index to access an access control list (ACL), wherein said ACL
4 includes information as to whether said packet can be sent via a tunnel.

1 15. The method of claim 14, wherein said information comprises:
2 an SGI field; and

3 a tunnel identifier field.

1 16. The method of claim 10, further comprising:
2 forwarding said packet from an ingress router to an egress router via a tunnel.

1 17. The method of claim 16, further comprising:
2 receiving said packet at said egress router; and
3 determining whether said packet can be forwarded by said egress router based
4 on said SGI.

1 18. The method of claim 17, wherein said determining whether said packet
2 can be forwarded further comprises:
3 determining whether said packet can be forwarded by said egress router based
4 on said SGI, a destination of said packet and an identifier of said
5 tunnel.

1 19. The method of claim 17, wherein said determining whether said packet
2 can be forwarded further comprises:
3 generating an index into an access control list (ACL), wherein
4 said ACL comprises information regarding whether said packet can be
5 forwarded by said egress router, and
6 said index includes said identifier of said tunnel; and
7 accessing said ACL using said index.

1 20. A computer system comprising:
2 a processor;
3 computer readable medium coupled to said processor; and
4 computer code, encoded in said computer readable medium, configured to
5 cause said processor to:
6 assign a security group identifier (SGI) to a packet; and
7 classify said packet based on said SGI.

1 21. The computer system of claim 20, wherein said computer code
2 configured to cause said processor to classify said packet generates a classification of
3 said packet, and said computer code is further configured to cause said processor to:
4 determine whether said packet can be sent via a tunnel based on said
5 classification.

1 22. The computer system of claim 21, wherein said computer code is
2 further configured to cause said processor to:
3 determine a routing of said packet, wherein said classification is also based on
4 said routing.

1 23. The computer system of claim 22, wherein said computer code is
2 further configured to cause said processor to:
3 forward said packet via said tunnel, if forwarding a packet having said SGI via
4 said tunnel is permitted.

1 24. The computer system of claim 21, wherein said computer code
2 configured to cause said processor to determine is further configured to cause said
3 processor to:
4 generate an index, wherein said index comprises said SGI; and
5 use said index to access an access control list (ACL), wherein said ACL
6 includes information as to whether said packet can be sent via a tunnel.

1 25. The computer system of claim 24, wherein said information comprises:
2 an SGI field; and
3 a tunnel identifier field.

1 26. The computer system of claim 20, wherein said computer code is
2 further configured to cause said processor to:
3 forward said packet from an ingress router to an egress router via a tunnel.

1 27. The computer system of claim 26, wherein said computer code is
2 further configured to cause said processor to:
3 receive said packet at said egress router; and
4 determine whether said packet can be forwarded by said egress router based on
5 said SGI.

1 28. The computer system of claim 27, wherein said computer code
2 configured to cause said processor to determine whether said packet can be forwarded
3 by said egress router is further configured to cause said processor to:
4 determine whether said packet can be forwarded by said egress router based on
5 said SGI, a destination of said packet and an identifier of said tunnel.

1 29. The computer system of claim 27, wherein said computer code
2 configured to cause said processor to determine whether said packet can be forwarded
3 by said egress router is further configured to cause said processor to:
4 generate an index into an access control list (ACL), wherein
5 said ACL comprises information regarding whether said packet can be
6 forwarded by said egress router, and
7 said index includes said identifier of said tunnel; and
8 access said ACL using said index.

1 30. A computer program product comprising:
2 a first set of instructions, executable on a computer system, configured to
3 assign a security group identifier (SGI) to a packet;
4 a second set of instructions, executable on said computer system, configured to
5 classify said packet based on said SGI; and
6 computer readable media, wherein said computer program product is encoded
7 in said computer readable media.

1 31. The computer program product of claim 30, wherein said second set of
2 instructions is further configured to generate a classification of said packet, and
3 further comprising:

4 a third set of instructions, executable on said computer system, configured to
5 determine whether said packet can be sent via a tunnel based on said
6 classification.

1 32. The computer program product of claim 31, further comprising:
2 a fourth set of instructions, executable on said computer system, configured to
3 determine a routing of said packet, wherein said classification is also
4 based on said routing.

1 33. The computer program product of claim 32, further comprising:
2 a fifth set of instructions, executable on said computer system, configured to
3 forward said packet via said tunnel, if forwarding a packet having said
4 SGI via said tunnel is permitted;

1 34. The computer program product of claim 31, wherein said third set of
2 instructions comprises:
3 a first subset of instructions, executable on said computer system, configured
4 to generate an index, wherein said index comprises said SGI; and
5 a second subset of instructions, executable on said computer system,
6 configured to use said index to access an access control list (ACL),
7 wherein said ACL includes information as to whether said packet can
8 be sent via a tunnel.

1 35. The computer program product of claim 34, wherein said information
2 comprises:
3 an SGI field; and
4 a tunnel identifier field.

1 36. The computer program product of claim 30, further comprising:
 2 a third set of instructions, executable on said computer system, configured to
 3 forward said packet from an ingress router to an egress router via a
 4 tunnel.

1 37. The computer program product of claim 36, further comprising:
 2 a third set of instructions, executable on said computer system, configured to
 3 receive said packet at said egress router; and
 4 a fourth set of instructions, executable on said computer system, configured to
 5 determine whether said packet can be forwarded by said egress router
 6 based on said SGI.

1 38. The computer program product of claim 37, wherein said fourth set of
 2 instructions comprises:
 3 a first subset of instructions, executable on said computer system, configured
 4 to determine whether said packet can be forwarded by said egress
 5 router based on said SGI, a destination of said packet and an identifier
 6 of said tunnel.

1 39. The computer program product of claim 37, wherein said fourth set of
 2 instructions comprises:
 3 a first subset of instructions, executable on said computer system, configured
 4 to generate an index into an access control list (ACL), wherein
 5 said ACL comprises information regarding whether said packet can be
 6 forwarded by said egress router, and
 7 said index includes said identifier of said tunnel; and
 8 a second subset of instructions, executable on said computer system,
 9 configured to access said ACL using said index.

1 40. An apparatus comprising:
 2 means for assigning a security group identifier (SGI) to a packet; and
 3 means for classifying said packet based on said SGI.

1 41. The apparatus of claim 40, further comprising:
2 means for determining whether said packet can be sent via a tunnel on based a
3 result generated by said means for classifying said packet.

1 42. The apparatus of claim 41, further comprising:
2 means for determining a routing of said packet, wherein said result is also
3 based on said routing.

1 43. The apparatus of claim 42, further comprising:
2 means for forwarding said packet via said tunnel, operable if forwarding a
3 packet having said SGI via said tunnel is permitted.

1 44. The apparatus of claim 41, wherein said determining comprises:
2 means for generating an index, wherein said index comprises said SGI; and
3 means for using said index to access an access control list (ACL), wherein said
4 ACL includes information as to whether said packet can be sent via a
5 tunnel.

1 45. The apparatus of claim 44, wherein said information comprises:
2 an SGI field; and
3 a tunnel identifier field.

1 46. The apparatus of claim 40, further comprising:
2 means for forwarding said packet from an ingress router to an egress router via
3 a tunnel.

1 47. The apparatus of claim 46, further comprising:
2 means for receiving said packet at said egress router; and
3 means for determining whether said packet can be forwarded by said egress
4 router based on said SGI.

1 48. The apparatus of claim 47, wherein said means for determining
2 whether said packet can be forwarded further comprises:
3 means for determining whether said packet can be forwarded by said egress
4 router based on said SGI, a destination of said packet and an identifier
5 of said tunnel.

1 49. The apparatus of claim 47, wherein said means for determining
2 whether said packet can be forwarded further comprises:
3 means for generating an index into an access control list (ACL), wherein
4 said ACL comprises information regarding whether said packet can be
5 forwarded by said egress router, and
6 said index includes said identifier of said tunnel; and
7 means for accessing said ACL using said index.